SYSTEM FOR PREVENTING UNAUTHORIZED ACCESS TO SENSITIVE DATA AND A METHOD THEREOF

ABSTRACT OF THE DISCLOSURE

A method and system for prevention of unauthorized access to multimedia data are disclosed herein. A tamper-resistant system having a software driver, a peripheral device, and a system memory is used to encrypt sensitive routines used by the software driver. The software driver is used to interface between one component of the system, such as a processor, and a peripheral device, such as a graphics chip. The driver incorporates one or more sensitive routines, that if divulged, could possibly allow an unauthorized party access to data processed by the software driver. Accordingly, in one embodiment, the sensitive routines are stored in an encrypted format with the driver. To access a sensitive routine, the driver submits the associated encrypted routine to the peripheral device, as well as a decryption method, if desired, where it is decrypted and stored in a plaintext format in a location, such as system memory, accessible to both the driver and the peripheral device. The driver can then use the plaintext routine to process the data. When finished processing the data, the plaintext routine can be re-encrypted using one or more of a variety of encryption methods and stored with the driver. Any remaining copies of the plaintext routine can be removed from the system. By encrypting the sensitive routines at all times other than when in immediate use, the system can effectively prevent an unauthorized party from accessing data based on knowledge about the sensitive routine. In addition, the use of the hardware of the peripheral device to encrypt/decrypt the sensitive routines provides an additional barrier to an unauthorized party.